This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2020.DOI

Improving Data Security, Privacy, and Interoperability for the IEEE Biometric Open Protocol Standard

EDUARDO M. DE LACERDA FILHO[1], GERALDO P. ROCHA FILHO[2], RAFAEL TIMÓTEO DE SOUSA, JR.[1] (Senior Member, IEEE), and VINÍCIUS P. GONÇALVES[1]

[1]National Science and Technology Institute on Cybersecurity, Electrical Engineering Department, University of Brasília (UnB), P.O. Box 4466 Brasília–DF, Brazil, CEP 70910-900 (e-mail: emlacerdaf@gmail.com, desousa@unb.br, vpgvinicius@unb.br)

[2]Computer Science Department, University of Brasilia - Brazil, 70910-900 (e-mail: geraldof@unb.br)

Corresponding author: Eduardo M. de Lacerda Filho (e-mail: emlacerdaf@gmail.com).

This work was supported in part by CAPES – Brazilian Higher Education Personnel Improvement Coordination (Grants PROAP PPGEE/UnB, 23038.007604/2014-69 FORTE, and 88887.144009/2017-00 PROBRAL), in part by CNPq – Brazilian National Research Council (Grants 312180/2019-5 PQ-2, BRICS2017-591 LargEWiN, and 465741/2014-2 INCT on Cybersecurity), in part by FAP-DF – Brazilian Federal District Research Support Foundation (Grant 0193.001366/2016 UIoT, and Grant 0193.001365/2016 SSDDC), in part by the Brazilian Ministry of the Economy (Grant 005/2016 DIPLA, and Grant 083/2016 ENAP), in part by the Institutional Security Office of the Presidency of Brazil (Grant ABIN 002/2017), in part by the Administrative Council for Economic Defense (Grant CADE 08700.000047/2019-14), and in part by the General Attorney of the Union (Grant AGU 697.935/2019).

ABSTRACT Enhancing security, privacy, and interoperability of biometric networks and protocols has been a challenge for many research works for many years. The several proposed approaches still need to integrate these three characteristics while showing security evidence for biometric applications. Therefore, this paper proposes a probabilistic scheme to encrypt biometric database indexes and a novel approach to interoperability among systems interchanging biometric characteristics, thus enhancing the IEEE Biometric Open Protocol Standard (BOPS). We highlight two meaningful improvements in our research when compared to related works. The first one comes from the proposed cryptographic techniques and network schemes. It implies a negligible probability for known attacks to be successful against the proposal, due to its semantic security evidence, as well as the difficulties that it imposes to the attacks, given the high complexity barriers that are unfeasible for the attacker to break in polynomial time, including the modified initialization vector and the nonce for the encryption algorithm. The second improvement comprises the new integrity and control procedures for biometric identification requests that boost the IEEE BOPS' reliability and contribute to interoperability purposes. The security analysis, proofs, and results demonstrate that the new proposed biometric network is faultless regarding integrity and interoperability while preserving the anonymity of persons whose biometric data is exchanged in the network and stored in the related databases.

INDEX TERMS Biometric, communication protocol, encryption, interoperability, privacy, security.

I. INTRODUCTION

SECURITY, privacy, and interoperability are three challenging biometric networks goals. Biometric Service Providers (BSP), which are the entities that provide biometric services on the network, are used by government services, banks, trade associations, and health departments, among other areas [1]. In this scenario, a sector uses different technological systems without a security and privacy interaction between the data or otherwise uses the same technique. Also, insecure and compromised biometric networks and databases can irreversibly lead to identity theft, unless they are properly security proof. In light of growing privacy concerns with regard to data usage, countries enacted laws to protect personal data by imposing solutions to mitigate the problem of attacks and data leaks [2], [3].

For many years, the main approach adopted to ensure biometric networks' security and privacy was applying biometric template techniques [1], [4]–[8]. The work of Ross *et al.* [9] pushes a lot of achievements to deal with template protection using biometric cryptosystems [10]–[17] and cancelable biometric (feature transformations) [18]–[21]. Some of these works also address authentication, network security, privacy data, and processing power. Unfortunately, some of them also have a few drawbacks [22]–[27]. Moreover, even with the guidelines of the IEEE Biometric Open Protocol Standard (IEEE BOPS) [28], it is not possible to use each of these schemes in different biometric databases and make them communicate in a way that is reasonably security proof and does not compromise a person's privacy. In addition, IEEE BOPS does not have a message exchange that allows an integrity check of transactions within the biometric network.

The problem then lies in enabling different biometric networks to communicate, with integrity, while ensuring individual data security and privacy. This proposed work resolves this problem by taking the following measures: introducing a probabilistic encryption scheme, conducting complete security analysis and evaluation, and establishing a set of new and complete communication protocols to improve the IEEE BOPS framework. The evidence shows that it is not feasible for the cryptographic techniques used to encrypt all the records in the BSP network and databases to be broken down in polynomial time and still preserve a person's anonymity. This research also compares other biometric cryptosystems and feature transformation methods with the IEEE BOPS framework, and this shows the innovative aspects of this paper more clearly. The contributions of this work are summarized as follows:

(1) A probabilistic encrypted index scheme to address data security and privacy.

(2) Using contribution (1), a new API to improve the workflow of IEEE BOPS [28], by enhancing the integrity and control of the exchanged data.

The first contribution runs an algorithm that creates an anonymous index called IDN. It uses a secret key (`k`), unique social identification of a citizen (`CPF`), and a Time Code Number (`TCN`). The IDN uses the AES-256-CBC encryption scheme [29], slightly modified by a random, secure, and local initialization vector (`iv`) and a `nonce` parameters. Using their own certified Federal Information Processing Standard (FIPS) [30] HSM, embedded in an audit environment, the different accredited BSP in the network can calculate and verify the same IDN string that represents the holder (`CPF`) of that biometrics unequivocally, without exchange `iv` or the `nonce`. The algorithm's goal is to ensure any person's anonymity with secure evidence, including semantic security, given by the probabilistic outcomes that prove and maintain this condition.

Our second contribution creates a new interoperability protocol to improve the IEEE BOPS API. The new proposal creates an API based on HyperText Transfer Protocol Secure (HTTPS) [31], and JavaScript Object Notation (JSON) [32] messages. The new API ensures interoperability and integrity between the biometric systems by exchanging the index (IDN). It is important to notice that IDN, within the network exchange and the databases, is not decrypted anytime. The security evidence of the network procedures and results proves that the protocol is secure enough to interoperate any biometric package within the BSP.

The rest of this paper has the following parts. Section II discusses the related works more comprehensively and examines aspects of security, privacy, and interoperability. We put forward the new scheme in Section III. In Sections IV and V, we conduct a security analysis and show the results of a running instance of the established framework. Finally, in Section VI, we summarize our paper's conclusions and make recommendations for future work.

II. RELATED WORK

Several studies currently investigate the security, privacy, and interoperability of biometric records. We will comment on some techniques that can enhance biometric protection, but to the best of our knowledge, none of them has been able to integrate security proofs, privacy, and interoperability simultaneously, as is the case with this research. Demonstrating how this problem of biometric data leakage is an issue in a given population, research conducted by Li and Zhang [33] showed that almost 80% of the participants were afraid that personal biometric information is liable to be stolen after being used in verification applications. Only 17% thought the verification carried out in the banking application was safe. About interoperability, some reasonable attempts at standardization have already been made [28], [34], and, as a further contribution made by our work, we will suggest a means of improving the IEEE BOPS framework.

A. SECURITY AND PRIVACY FEATURES

Some factors need to be taken into account when seeking to make biometrics networks and databases secure and ensure data privacy. The work on differential privacy carried out by Dwork [34] showed that there is a great deal of auxiliary information that an attacker can obtain without accessing the database. Thus, it is essential to narrow down our understanding of what research is required to establish security and privacy. Our work is clear about these goals, *i.e.*, it is to enhance data security and privacy within the parameters of the biometric network and database, using cryptographic techniques based on security evidence.

B. BIOMETRIC SECURITY AND PRIVACY WORKS

Parts I and II from Lai *et al.* [16], [17] set out some fundamental theories. The authors describe the trade-off among security, privacy, and key protection in any biometric (template) security system when a single-use case of biometrics and when facing the reuse of the same biometric information in multiple locations. The works deal with specifics biometric measurements for different approaches when generating the key in biometric authentication systems: (a) non-randomized approach; (b) randomized approach.

Nagar *et al.* [15] proposes a feature-level fusion framework. It bases on a transformation embedded algorithm which makes a biometric feature x_m into a new binary or commitment/vault representation z_m, a fused module that combines homogeneous biometrics and a biometric cryptosystem that generates a secure sketch in the enrollment

IEEE Access

procedures. The proposed work presents some security analysis for the created biometric template and improving performance.

The work of Nassir and Perumal [14] uses the user ID and password with the biometric data extracted, converted to decimal numbers. When using symmetric and RSA algorithms, the work encrypts and signs the data into one package. At the database, they decrypted this packet for decision analysis. The work shows some performance evaluation without security analysis.

Rathgeb *et al.* [20] work proposes a Bloom filter-based transforms to protect templates in face and iris samples. It builds two matrices arranged in two-dimensional binary code, divided into blocks of equal size consisting of $w_F(w_I)$ bits. The transform h applies to map the binary column to its equivalent decimal value, which locations were within the Bloom filters. A hash function applies leading face and iris to had the same transform length, and, in the last step, the transformed face and iris are bit-wise fused to improve privacy.

The paper from Kumar and Kumar [12] proposes a multimodal biometric cryptosystem based on two modes: (a) feature-mode; (b) decision-mode. The construction consists of three phases, *i.e.*, a Bose Chaudhuri Hocquenghem (BCH) applied in the biometrics, creating parity-code, a locking stage hash-code computation performed on the biometric modalities, and the unlock stage where the parity-code regenerates using XOR-coding. The experimental analysis confirms the superiority of multimodal cryptosystems and decision-level fusion.

Li *et al.* [13] describes a new security analysis, proposing a multibiometric construction by using a fingerprint to encrypt the key. By combining information-theory and security, the work uses triangulations, features extraction, and two levels of encryption, one with hash functions and fuzzy vaults to bind the transformed fingerprint template and the other with Shamir's secret sharing scheme to split and store the hash values. A decision-level fused obtains the identity of a sample.

Kaur and Sofat [35] fuzzy vault work incorporates a fuzzy vault multimodal biometric template approach. The fuzzy vault is a combination of extracted minutia points fingerprint and face using crossing number and principle component analysis, where the fused is the input vault, for encoding, and Lagrange interpolation to recover the vault key, for decoding. The proposed scheme shows that the approach yielded satisfactory performance and provides the claimed security.

Zhou and Ren [11] work proposes a Threshold Predicate Encryption (TPE) using a functional encryption scheme. An encrypted plaintext and a secret key associate with a vector, using Inner Product Encryption and Predicate Encryption instances that leave the decryption a function value and not the plaintext anymore. No sensitive information about the vectors could not be passive or active attacks.

Toli and Preneel [10] work uses a pseudo-identity authentication recorder of a bank's client. With a client's PIN code, the device encrypts and stores the package, discarding the biometrics and the PIN. For security requirements, the proposal uses ISO biometric, financial, and cryptographic device standards.

Kaur and Khanna [18] proposes a random distance method. Considering the multimodal cancelable biometric template approach, it generates a *discriminative and privacy-preserving revocable pseudo-biometric identities*. According to the user secrecy, the method mapped, on the Cartesian space, biometrics features, and calculates the distance for some points. The security analysis presents some resistance to known attacks.

C. THE IEEE BOPS FRAMEWORK

The ANSI/NIST packages [36], and IEEE BOPS API [28] reference the interoperability of components within different biometric systems. It should be noted that there are studies that attempt to establish interoperability mechanisms, such as Tolosana *et al.* [37] and Mason *et al.* [38]. However, no comparative study will be made of them in this paper because they are only concerned with biometric devices and data, but not all the transaction workflow. We describe the IEEE BOPS, owing to the improvement made by our scheme to this framework.

The IEEE BOPS assures multilevel access control, identity claim, auditing process, and enables interoperability independent of the underlying system. The proposed architecture is built for pluggable components using neutral languages, such as Representational State Transfer (REST), JSON, and Transport Layer Security/Secure Sockets Layer (TLS/SSL) [28], providing a client/server communication interface. The BOPS mechanism includes software, a trusted BOPS Server, and Intrusion Detection System. The BOPS uses an API for interoperability purposes that will be the subject of this paper.

Sections 6 through 9 of the IEEE BOPS document describe the interoperability considerations, including the API format. The API runs a 2-way SSL certificate dealing with replay attacks, controls the authentication procedures, and JSON messages among the BOPS server and the client device. It creates five types of procedures (Assertion, Role Gathering, Multi-Level Access Control, Assurance, and Auditing) that hold the communication by a triple association of user, device, and session.

The API starts with a JSON error code message for connection calls. Afterward, the BOPS documentation describes JSON messages about initial setup, devices, and session authentication - by certificate exchange -, and communication security, including a "QROpportunity" that identifies the client application. The Role Gathering part includes a descriptive flow of input and output parameters about the session's construction, creation, status, data, and termination. Between the status and data session is where biometrics are enrolled and sent to the network. The control mechanism triggers a binary response for the "JSONObject", that includes,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

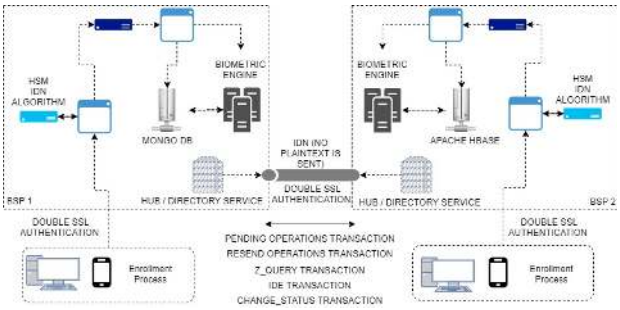


Figure 1. The implemented architecture.

or not, the data returned related to the security connection issue. Finally, the API proposes an assurance and auditing JSON messages for group actions (read/write) on any set of data.

Although BOPS deals with details on security and authentication, the problem lies in the fact that IEEE BOPS has no effective integrity mechanism *i.e.*, between the status and data session in the Role Gathering. The multi-level control does not offer acknowledged messages about the object of biometric transactions. It does not include dealing with the pending operations, time-out, or bad connection recovery among systems for the biometric identification procedure. Our research uses the ANSI/NIST package and proposes an integrity subsection in the API documentation, improving IEEE BOPS.

III. THE PROPOSED SCHEME

In this section, we outline the following:

- The probabilistic encrypted IDN scheme.
- How the secret key is protected.
- The proposal to insert a subsection in the IEEE BOPS API documentation.
- An extensive comparison of our work and others regarding security, privacy, and interoperability.

Figure 1 represents the implemented architecture. It shows that the IDN algorithm runs on the HSM of each BSP, after the enrollment process. That same HSM is where the secret key is protected. It also presents the interoperability calls that occur between BSP, and, as will be shown, it can be within the IEEE BOPS documentation.

A. THE IDN

The IDN generation scheme, shown in Algorithm 1, uses the social number `CPF`, the Time Code Number `TCN`, and the secret key `k`, as follows:

- The `CPF` is expanded by concatenation by itself until it gets a 256-bit length;
- The `iv` parameter is calculated by concatenation of `k` and `CPF` expanded, resulting 512-bit string called `y`; then, we get `x` by applying `x` = SHA256(`y`), a 256-bit string; after, we divide `x` in two halves, letting `a` be the first 128 bits and `b` the trailing ones; and finally `iv` = `a`⊕`b`;
- The `CPF` is padded until it gets 128 bits and it is AES-256-CBC encrypted using `k`, feasible to be calculated for the BSP, but with a unknown `iv` for an adversary A, as the `iv` is not transmitted over the network. This yields `z`, an encrypted 128-bit string;
- The `nonce` parameter is calculated similarly as `iv`, *i.e.*, the `TCN` is shrunken for 256-bit string, then concatenated with `k`, resulting 512-bit string called `u`; then, we get `v` by applying `v` = SHA256(`u`), a 256-bit string; after, we divide `v` in two halves, letting `c` be the first 128 bits and `d` the trailing ones; and finally `nonce` = `c`⊕`d`;
- At last, IDN = `z`⊕`nonce`, feasible for only the BSP to reverse, finding the same `z` for any tuple IDN and `TCN`, since IDN and `TCN` are the only parameters to be exchanged in the network.

Algorithm 1: IDN algorithm

Data: CPF, k, TCN
Result: IDN
Read the value of k;
Read the value of CPF;
Read the value of TCN;
$k \in \{0,1\}^{256}$;
$CPF \in \{0,1\}^{88}$;
$TCN \in \{0,1\}^{288}$;
x^j is the j^{th}-bit of x;
h^j is the j^{th}-bit of h;
v^j is the j^{th}-bit of v;
foreach *CPF* **do**
  $CPFEXT = CPF||CPF||CPF \in \{0,1\}^{256}$
  $y = k||CPFEXT \in \{0,1\}^{512}$
  $H \xrightarrow{y} x$
  $a \in (x^0, x^1, ..., x^{127})$
  $b \in (x^{128}, x^{129}, ..., x^{255})$
  $iv = a \oplus b$;
  $AES\text{-}256\text{-}CBC(CPF, iv, k) \rightarrow z$
  $TCN \in (h^0, h^1, ..., h^{255})$
  $u = k||TCN \in \{0,1\}^{512}$
  $H \xrightarrow{u} v$
  $c \in (v^0, v^1, ..., v^{127})$
  $d \in (v^{128}, v^{129}, ..., v^{255})$
  $nonce = c \oplus d$
  $IDN = z \oplus nonce$
end foreach
Return IDN

The same `CPF`, when enrolled at different times, it will generate distinct IDN, because each transaction have a different TCN_i. However, the same `CPF` enrolled, *e.g.*, at different times, resulting the tuples $IDN_1//TCN_1$ and $IDN_2//TCN_2$, will generate the same `z`, as follows:

- Computes `nonce` with TCN_i;
- Do $IDN_i \oplus nonce$ resulting `z`.

Algorithm 2: z algorithm

Data: IDN$_i$, TCN_i
Result: z
Read the value of IDN$_i$;
Read the value of TCN$_i$;
v^j is the j^{th}-bit of v;
foreach TCN_i **do**
  $u = k||TCN_i \in \{0,1\}^{512}$
  $H \xrightarrow{u} v$
  $c \in (v^0, v^1, ..., v^{127})$
  $d \in (v^{128}, v^{129}, ..., v^{255})$
  $nonce = c \oplus d$
  $z = IDN_i \oplus NONCE$
end foreach
Return z

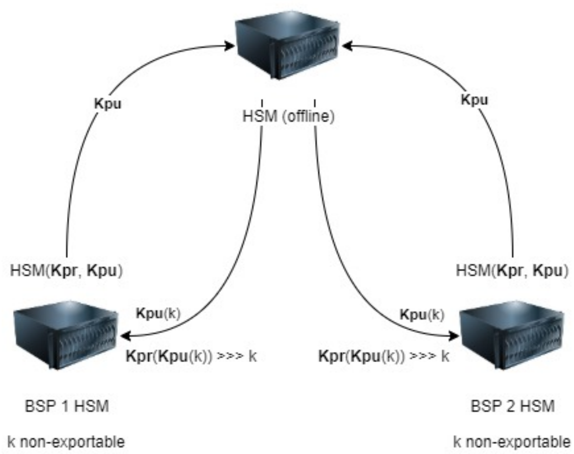


Figure 2. Life-cycle and security of the secret key k.

Using Algortithm 2, if z is the same, *e.g.*, for the stored tuple $IDN_1//TCN_1$ and the incoming tuple $IDN_2//TCN_2$, it means that it is the same CPF. Only the BSP that have k, CPF and TCNi can reach the same z for the same CPF. All those cryptographic calculations are done within the cryptographic module of each BSP HSM.

B. SECRET KEY LIFE-CYCLE AND PROTECTION

We will describe how this proposal deals with the life-cycle and protection of the secret key k. For generation purposes, we create a 256-bit random k into an offline HSM. After creating it, we export k by using RSA-OAEP encryption operations, with the public keys (Kpu) of the BSP HSMs in the network. This procedure produces only one cryptographic envelope (Kpu(k)) per each BSP HSM, containing the secret key k. Only the private key (Kpr) of each BSP can decrypt the envelope (Kpr(Kpu(k))). The security of these operations it is in section IV. Figure 2 shows the workflow of the life-cycle of the k.

To export and import the secret k (Secret_2.key), we use the following commands, shown via OpenSSL script, with RSA-OAEP-2048-bit padding [39], [40]:

Input: "Certificate_from_BSP.cer", "Secret_2.key"
Output: key.key
Initialization:
$ openssl x509 -pubkey -noout -in Certificate_from_BSP.cer > HSM_.pub -inform DER;
$ openssl rsautl -oaep -encrypt -inkey HSM_.pub -pubin -in Secret_2.key -out Key.key;

Input: "HSMprivate_.key", "Key.key"
Output: Secret_2.key
Initialization:
$ openssl rsautl -oaep -decrypt -inkey HSMprivate_.key -pubin -in Key.key -out Secret_2.key;

A local audit ceremony imports k into the BSP HSM with the feature "non-exportable". It is not possible, with this procedure, to copy or export k. The FIPS test certification requirements [30] guarantees this HSM non-exportable tool. The conditions established in the FIPS tests documentation also deal with HSM's inviolability against penetration, side-channel, physical, chemical, and other attacks. Indeed, one of the premises is that a certified HSM by internationally recognized mechanisms, *e.g.*, FIPS, is necessary for our proposal. All of these tools and procedures address the protection of the secret key k from violations and attacks.

C. THE NEW PROPOSAL FOR IEEE BOPS API DOCUMENTATION

In this subsection, we will describe the API created to improve the proposal in the IEEE BOPS documentation. As reported, the IEEE BOPS API, between "sessionstatus" and "sessiondata", does not have messages that guarantee client/server biometric data transactions' integrity. We suggest inserting a subsection about "Integrity", including a session called "sessionIntegrity", between "sessionstatus" and "sessiondata", in the Role Gathering procedure, considering the following commands. Our API has two different approaches for HTTPS messages and five JSON transactions that improve the IEEE BOPS framework. We are going to describe each of them. Please refer to Appendix B for more details about the new API.

1) HTTPS messages

We propose two different services for the suggested session protocol, *i.e.*, for the IEEE BOPS API Role Gathering part. The first one is the *HUB service* that takes care of the asynchronous transactions, *i.e.*, biometric identifying (1:n), or verifying (1:1) transactions between client and BSP or BSP to other BSP. The second one is the *Directory service* that takes care of the synchronous transactions, *i.e.*, bad connection responses, pending operations, time out, among others.

The *HUB service* follows the asynchronous pattern, *i.e.*, all responses must be returned by the HUB that received the request when it has the available information. All requests

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

transaction in *HUB service* must use the POST method, with the ANSI/NIST biometric file in the request body, and must contain the following headers:

```
NIST/XML: Content-Type: application/xml
NIST/binary Content-Type: application/
octet-stream
```

The *Directory service* follows the synchronous pattern, *i.e.*, all responses must be returned in the same request/response. A reliable source of time synchronizes BSPs. All requests transaction in *Directory service* must use the POST method, and must contain the following headers:

```
Accept: application/json
Content-Type: application/json
```

The response headers must contain the following parameters:

```
Content-Type:  application/json
```

In Section V we will show the *HUB service* and *Directory service* working in the BSP network proposed for this work.

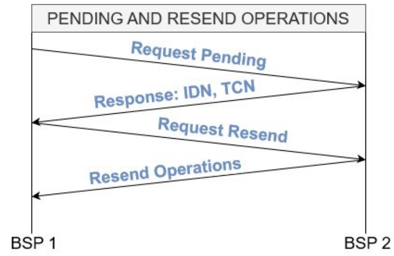


Figure 3. Sequence of events to list pending operations between BSP.

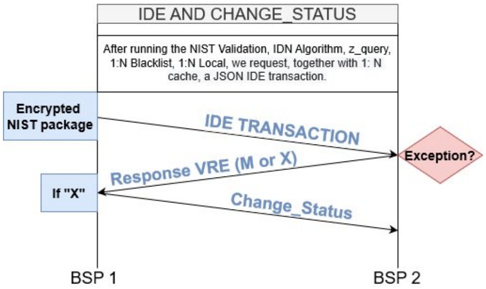


Figure 4. IDE and change_status notification transactions.

2) JSON messages

We will describe the JSON messages that create an integrity mechanism in IEEE BOPS API documentation. As is done in Section 9 of the IEEE BOPS, we will explain the integrity mechanisms created, and, in the API shown in Appendix B, we show the calls (request/response) in JSON. Figures 3 and 4 present the workflow for these messages in the network proposed. Please refer to Appendix B for more details.

a. JSON pending operations listing transaction (Figure 3). In case of an incident with a client or a BSP, *e.g.*, timeout, bad-connection, or maintenance, the transaction shows a list of IDN and TCN (indexes created in this work, but could be any other) that requires further processing that could not be done on-line. After, the BSP requests the other to resend the missing operation, only for IDNs that were not locally processed. Hourly, the procedure sends a JSON type to ensure that all processes have been executed, holding integrity through the network.

b. JSON resend transaction (Figure 3).
After receiving the pending IDN list, the BSP asks what operations should be performed. This JSON message assures that the client or the BSP knows what was the missing transaction and enforce to operate the task.

c. JSON z_query transaction
This transaction intends to ask if a z code, shown in Algorithm 2, is registered within the BSP local and cache database. As reported, the z parameter was created for this work, but it could be any indexer on a biometric basis. The same registered z is a JSON message response with a TRUE|FALSE for existing or not. If z exists, it figures out which fingerprints and face are registered (TRUE|FALSE), along with the related IDN_i and TCN_i.

d. JSON IDE transaction (Figure 4) A JSON message allows clients and servers to perform an identification or verification operation in the biometric network. Client to BSP, or BPS to BSP, sends an IDE transaction. The IDE transaction is the other (remote) entity's command to begin the identification or verification process. It has attached the encrypted ANSI/NIST package that can only be opened by a particular BSP, which has the corresponding private key for additional security regarding the network. The response is a VRE transaction with the value M or x.

e. JSON change status notification transaction (Figure 4). It is an acknowledgment JSON message for the client or the BSP, showing an identification process's termination status. For this proposal, it ensures that BSP can store the tuple IDN and TCN, associated with the biometrics, in the database.

D. COMPARISON AMONG RELATED WORKS

Few techniques like our work refer to the security evidence and anonymity of the index register into biometric databases. In Table 1, we show an informative outline of the existing approaches. It is possible to realize that features transformations and cryptographic techniques among biometrics systems are not new. However, up to our best knowledge, it had not been used to hold privacy with security evidence, and also, creating an interoperability protocol between different biometric database systems.

IEEE BOPS framework does not have any JSON messages that allow the client device to know, with integrity and possibility of recovery, the biometric transactions. Our research, shown in Table 2, improves IEEE BOPS by constructing JSON messages that allow the interoperability and integrity of biometric transactions, pointing out if one did not

Table 1. Summary of related works compared to the proposed framework. Security, privacy and interoperability aspects were considered.

Works	Security and privacy biometric data approach	Security and privacy biographical data approach	Security against known attacks	Interoperability
Lai *et al.* [16]	YES	NO	YES	NO
Lai *et al.* [17]	YES	NO	YES	NO
Nagar *et al.* [15]	YES	NO	YES	NO
Nassir and Perumal [14]	YES	YES	NO	NO
Rathgeb *et al.* [20]	YES	NO	YES	NO
Kumar and Kumar [12]	YES	NO	YES	NO
Li *et al.* [13]	YES	NO	YES	NO
Kaur and Sofat [35]	YES	NO	NO	NO
Zhou and Ren [11]	YES	NO	YES	NO
Toli and Preneel [10]	YES	YES	NO	NO
Kaur and Khanna [18]	YES	NO	YES	NO
Our proposed scheme	**YES**	**YES**	**YES**	**YES**

Table 2. Comparison among IEEE BOPS framework and our research.

Works	Security channel	API Interoperability	Integrity	Recovery
IEEE BOPPS [28]	YES	YES	NO	NO
Our proposed scheme	**YES**	**YES**	**YES**	**YES**

complete the purpose task. Also, it allows us to use the IDN algorithm created, ensuring the anonymity of the records.

IV. SECURITY ANALYSIS

We divide this section into three areas of security analysis. The first and the second are focused on cryptoanalysis, mainly on the randomness of the secret key [41], semantic security (SS) [42], forward by indistinguishability (IND) notation security [43]. The third one is based on network operations security. For the security definitions of this paper, Non-malleability (NM) implies IND, but for adaptive Chosen Ciphertext Attack (CCA2), IND also implies NM [43]. SS is equivalent to IND in Chosen Plaintext Attack (CPA) model [42], but not in CCA models [43].

A. THE SECRET KEY IS RANDOM NUMBER GENERATED

Lemma 1. *The k is Random Number Generated [41].*

Proof. Please refer to Appendix A. □

B. SS AND IND SECURITY

Definition 1 (CPF)**.** The `CPF` is given by:

$$CPF = (d_0; d_1; d_2; d_3; d_4; d_5; d_6; d_7; d_8; d_9; d_{10}),$$

where d_n is a decimal digit that is represented by one octet block. In the first eight positions of `CPF`, each octet block has 4-bit entropy. The ninth represents a Brazilian state position. The last two positions are checkers, completing eleven digits, and are calculated according to the first nine and ten, *i.e.*, $d_9 = ((\sum_{i=0}^{8} d_i * (i+1))mod11)mod10$; and $d_{10} = (((\sum_{i=0}^{9} d_i * i)mod11)mod10$.

Proposition 1. *IDN is secure against Birthday Attack [44], [45] and Biclique Attack [46] for any A.*

Proof. Towards proving that our encrypted IDN scheme is secure against the Birthday Attack and Biclique Attack, we must explain the novel, random, and locally calculated `iv` and `nonce` created. For `iv`, we begin concatenating the 88-bit `CPF` string until 256-bit length, with the 256-bit `k`, resulting in a 512-bit length. We use the entropy of a uniform random variable, independent SHA-256 to one way 256-bit string, converging to a $\log_2((1-1/e) \times 2^{256})$ entropy output effort. For `nonce` we concatenate the 256-most valuable bits `TCN` string with the secret `k`. We calculate the SHA-256 of this concatenation, leading to a 256-bit length. We achieve for `nonce` the same security level of the `iv` parameter.

The 128-bit `CPF` padded plaintext it is XOR-ed with a 128-bit random `iv` for every entrance, leading a random $blockCPF \in^{128}$. Instead of rebooting the encrypted AES-256-CBC with the previous outcome and an initialization vector, we XOR-ed the block entrance of the AES-256-CBC with a true 128-bit random, and local `iv`, derived from known parameters (`k` and `CPF`) only for the accredited BSP. This process leads our encryption scheme to a 256-bit entropy effort. The `nonce` is XOR-ed with the outcome of AES-256-CBC, resulting in IDN, leading a 128-bit entropy effort.

A cannot has control of the input bits calculated by XOR-ing the random `iv`, and also A cannot computes `nonce` parameter. The computational cost effort, for our IDN scheme, to find a collision is approximately $2^{n/2}$, n = 256 (`k`-bit), for birthday attacks. Moreover, the computational cost effort for a biclique key recovery is over 2^{250}-bit, under 14-rounds for 2^{40} data, and a preimage attack, it is over 2^{120}-bit, under 14-rounds [46]–[48]. Therefore, this computational effort leads to unfeasible known polynomial-time attacks between the plaintext `CPF` to the encrypted IDN or IDN to `CPF`, holding anonymity. □

Proposition 2. *IDN is secure against Chosen Ciphertext Attack - CCA - [49], Padding Oracle Attack - POA - [50], and Chosen Plaintext Attack - CPA [49], for any A.*

Proof. As definition, a well implemented AES-CBC is security against POA and CPA [49], [50], but not CCA, until our research. For a general CCA, an adversary A sends to the Oracle O a (m_1, m_2) plaintext block. After receiving $C_i = (IV, (IV \oplus m_i))$, A sends O, $C'_i = (IV \oplus t, (IV \oplus m_i))$ - t is a random string. By decrypting it, A obtains $((IV \oplus m_i)) \oplus IV \oplus t$ = $m_i \oplus t$. So, A calculates $(m_i \oplus t) \oplus t$ that leads to m_i. Now A can compare i with the original messages. In our work, the `iv` and `nonce` parameters are not sent over the network. They work only within the cryptographic module of the BSP HSM. Therefore, *e.g.*, $(\texttt{iv} \oplus t, AES\text{-}256\text{-}CBC(\texttt{iv} \oplus \texttt{CPF}))$ cannot be enforced by A. The same approach can be done for `nonce` parameter. The only information sent through the network (and stored in the databases) is IDN ciphertext and `TCN`. The calculations of `iv` and `nonce` in the IDN scheme are unfeasible for any A. □

Proposition 3. *The proposed PKE is SS [51], forward by PKE IND-CPA, IND-CCA, and IND-CCA2 notation [51], against any adversary A.*

Proof. The RSA-OAEP-2048-bit encryption scheme computes $s = (m||0^{k_1}) \oplus G(r)$ and $t = r \oplus H(s)$, outputing $c = f(s, t)$, where r is a k-bit integer random generated, f is a oneway trapdoor function of pk. The RSA-OAEP-2048-bit decryption scheme computes $(s, t) = g(c)$, where g is the inverse of f using sk, $r = t \oplus H(s)$, $M = s \oplus G(r)$. For k_1 LSB of M and n MSB of M, if $[M]_{k_1} = 0^{k_1}$, PKE algorithm returns $[M]^n$, otherwise "reject".

We use the RSA-OAEP-2048-bit padding encode framework, for the message m, in the cryptographic module of the HSM. Recovering a message $m \in \{0,1\}^*$, A must compute $r = Y \oplus H(X)$, $H : \{0,1\}^{k-k_0} \rightarrow \{0,1\}^{k_0}$ is the Random Oracle (RO), $Y = r \oplus H(X)$, and $X = G(r) \oplus m_{padded}$, where $G : \{0,1\}^{k_0} \rightarrow \{0,1\}^{k-k_0}$ is a RO. The encode framework gives $RSA - OAEP(m_b) = RSA(X||Y)$, where $b \in \{0,1\}$. Because OAEP does include a uniform random value in m_{padded}, A cannot recover $X||Y$, which relies on the hardness of RSA-2048-bit problem [39]. A cannot guess b and AdvA$[(k)]$ is negligible for CPA.

Assuming that y^* is a challenge ciphertext of m_b, r^* is a random integer and follows the same iteration of the Oracle OAEP encryption. For a not queried s by the RO $H(s)$, we have a uniform random distribution of $H(s)$, and $r = t \oplus H(s)$. So, there is a tiny probability that $t \oplus H(s)$ is queried by RO G or refers to r^*, leading to a random $G(r)$ and there is a minor probability that 0^{k_1} is computed, leading Oracle decryption rejects. By rejecting, A cannot combines the Oracle lists for a preimage of y, indicating that RSA-OAEP-2048-bit is IND-CPA, IND-CCA and also IND-CCA2 encryption scheme.

From the exposition, we can assume that our PKE is SS. The difficulty of inverting the high exponents RSA function and the RO security model, *i.e.*, under the assumption that the hash functions used in the scheme behave as RO, proves that our PKE scheme is secure, considering the note found in RFC 8017 [39]. We use SHA-256 [52] for our proposed scheme. Our RSA-OAEP-2048-bit implementation makes $AdvA[(k)]$ negligible. □

Other significant attacks and methods must be considered. For the AES-256-CBC algorithm, a related-key amplified boomerang attack has $2^{99.5}$-bit complexity, in 14 rounds for $2^{99.5}$ data [53]. The hardness of exploiting RSA-2048, using index calculus Number Field Sieve (NFS), has a 2^{112} complexity [54], [55]. The offline and BSP HSMs implement cryptographic calculations in a constant-time, with differential power analysis resistant cores and libraries embedded in a secure cryptographic module, accredited with FIPS test suite [30]. This approach avoids side-channels attacks, *e.g.*, timing attacks [26], [56], power analysis [57] and fault analysis [58].

C. NETWORK OPERATION SECURITY

We will comment on some possible attacks on devices and networks, pointing out the countermeasures for each of them. The wrapped `k` is imported in a local ceremony at the BSP's security environment. The offline HSM and BSP HSMs [30] have a feature that does not allow any copy or misuse of the non-exportable `k`. The root master administrator can only create or destroy the logical-space into the slot but will never gain the slot's ownership. The BSP HSMs have other security features embedded, *e.g*, multiple level authentication, split access among operators, Intrusion Detection System (IDS), non-physical, mechanical, chemical violability, and Structured Query Language (SQL) injection protection [30], [59].

Mutually authenticated channels for all communication is done using a TLS/SSL (RSA-2048-bit) [60]. By a signed trusted biometric service list, each accredited BSP IP and URL end-points are informed. There are dedicated firewalls that only set the route IP of each BSP. The biometric ANSI/NIST packages have the name of the issuing and the destination BSP. All names are retrieved from the certificate embedded in the trusted list. In addition to every network part mentioned, BSP uses time synchronization with a reliable time source with a timestamp for transaction exchange. From this exposure, replays attacks [61] and Distributed DoS attacks [62] can be mitigated.

V. RESULTS

We show the security evaluation of our work against known attacks and demonstrate the IDN scheme calculations. Finally, we present the new interoperability communication protocol, with the built API, working for an identification purpose (`IDE`) and the respective performance. All results were obtained using data acquired from the operating BSP network.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

A. SECURITY EVALUATION

Table 3 shows security evaluation of our proposed scheme. Based on Section IV, we show the complexity, the unfeasible mathematical approach, and the method applied for a negligible probability for each known attack.

Our work's main cryptographic contribution is the randomly calculated `iv` and `nonce` parameters. The `iv` and `nonce` have 128-bit length, and they are not sent through the network, working locally and re-calculated for each entrance. Consequently, A cannot predict, compute, or enforce in a polynomial-time the `iv` and `nonce`, thus repealing significant attacks against the IDN proposed scheme, including CCA against AES-256-CBC. The complexity of breaking the proposed encrypted IDN is not feasible in a polynomial-time attack. OAEP implementation's complexity relies on finding a collision in the RO $\leftarrow$ SHA-256 and in the hardness of breaking RSA-2048-bit. All storage and calculus are done in an accredited HSM that generates random `k`, applying side-channels countermeasures, with a non-exportable asset feature. The main result of our scheme is the enhanced security and privacy of biometric network and databases.

For network operation, ensuring the interoperability protocol, known practices have been implemented to repeal attacks. Mutually SSL communication channels with a signed BSP Trusted Certificate List, IPsec protocols, dedicated IP/URL endpoints, synchronized BSP, and timestamp message are some methods that can mitigate, *e.g.*, Distributed Denial of Service (DDoS) and replay attacks.

B. THE IDN

The IDN (an OpenSSL script):

Input: “CPF”, “TCN”, “Key.key”

Output: IDN

Initialization:

```
read CPF
read TCN
CPFhex=$(echo -n $CPF | xxd -p)
CPFEXT=“$CPFhex$CPFhex$CPFhex”
CPFEXT=“${CPFEXT:0:64}”
K=“$(echo $(hexdump -v -e ’/1 “%02X” ’ < Key.key))”
KCPF=“$K$CPFEXT”
KCPF=“${KCPF:0:128}”
shaX=$(echo -n $KCPF | xxd -p -r | sha256sum | cut -d ’
’ -f 1)
A=“${shaX:0:32}”
B=“${shaX:32:32}”
IV = “”
for ((i=0; i < ${#A}; i+=2 ))
do
Ai = $((16#${A:$i:2}))
Bi = $((16#${B:$i:2}))
xorAB = $(( Ai ^ Bi))
tmp = $(printf ’%02x’ $xorAB)
IV = “${IV}${tmp}”
done
lData=${#CPFhex}
lPadding=$(( (32 - $lData)/2 ))
blockCPF=“${CPFhex}”
tmp=$(printf ’%02x’ $lPadding)
for ((i=0; i < $lPadding; i++ ))
do
blockCPF=“${blockCPF}${tmp}"
done
z=$(echo -n $blockCPF | xxd -p -r | openssl enc -nopad -e
-a -nosalt -aes-256-cbc -K $K -iv $IV)
TCNhex=$(echo -n $TCN | xxd -p)
TCNEXT="${TCNEXT:0:64}"
KTCN="$K$TCNEXT"
KTCN="${KTCN:0:128}"
shaT=$(echo -n $KTCN | xxd -p -r | sha256sum | cut -d ’
’ -f 1)
C="${shaT:0:32}"
D="${shaT:32:32}"
NONCE=""
for ((i=0; i < ${#A}; i+=2 ))
do
Ci=$(( 16#$C:$i:2 ))
Di=$(( 16#$D:$i:2 ))
xorCD=$(( Ci ^ Di ))
tmpnonce=$(printf ’%02x’ $xorCD)
NONCE="${NONCE}${tmpnonce}"
done
IDN=""
for ((i=0; i < ${#A}; i+=2 ))
do
zi=$(( 16#${z:$i:2} ))
NONCEi=$(( 16#${NONCE:$i:2} ))
xorzNONCE=$(( zi ^ NONCEi ))
tmpidn=$(printf ’%02x’ $xorzNONCE)
IDN="${IDN}${tmpidn}"
done
```

Table 4 shows the IDN calculations for the proposed scheme created. Those are made, following the script, by using a possible (hypothetical) `CPF` and `TCN`, with a test key `k`, generated from the offline HSM, for experimental purpose. According to the results, `iv`, `nonce`, `z`, and IDN cannot be calculated without the knowledge of `k`, associated with `CPF` and `TCN`, *i.e.*, only BSP in the network are able to generate `z` for the same plaintext `CPF`. In the next subsection, we will show a real `CPF`, shown as IDN, in this operation biometric network.

C. THE NEW INTEROPERABILITY COMMUNICATION PROTOCOL

We present the results for the new interoperability communication protocol proposed. The logging trail was extracted from BSP1, showing communication between *Network 1* (BSP1) and *Network 2* (BSP2), with a real and irreversible IDN. The `pending_operation`, `operation_resend`, `z_query` and an `IDE` transactions

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

Table 3. Security Evaluation.

Attacks	Complexity	Probability	Applied Method
Birthday	$2^{256/2}$	$Pr \geq 0.5$	IDN algorithm 1
Related-Key Boomerang	$2^{99.5}$	$Pr = 1$	AES-256-CBC
Biclique	$\sim 2^{254}$; $\sim 2^{126}$	$Pr = 1$; $Pr = 0.63$	AES-256-CBC
CCA	2^{128}	$Pr = 1$	IDN algorithm 1
POA	2^{128}	$Pr = 1$	$OTP(\texttt{iv}) \oplus Plaintext(\texttt{CPF})$
CPA	2^{128}	$Pr = 1$	AES-256-CBC, with non-predictable and random `iv`; the resulting AES-256-CBC is XOR-ed with non-predictable and random `nonce`
IND-CPA	$2^{\log_2((1-1/e)\times 2^{256})}$; 2^{112}	$Pr \geq 0.5$; $Pr = 1$; $Adv^f_{A_{1,2}}[(k)] \sim$ negligible	RO $\leftarrow$ SHA-256; RSA-OAEP-2048
IND-CCA1	$2^{\log_2((1-1/e)\times 2^{256})}$; 2^{112}	$Pr \geq 0.5$; $Pr = 1$; $Adv^f_{A_{1,2}}[(k)] \sim$ negligible	RO $\leftarrow$ SHA-256; RSA-OAEP-2048
IND-CCA2	$2^{\log_2((1-1/e)\times 2^{256})}$; 2^{112}	$Pr \geq 0.5$; $Pr = 1$; $Adv^f_{A_{1,2}}[(k)] \sim$ negligible	RO $\leftarrow$ SHA-256; RSA-OAEP-2048
NFS	2^{112}	$Pr = 1$	RSA-2048
Timming	-	negligible	Constant-time
Power Analysis	-	negligible	DPA resistant cores and libraries
Fault Analysis	-	negligible	Fault Injection Prevention; Hardware and Time Redundancy; Operation Hiding; Blinding Infection; Protocol Protection
(D)DoS	-	negligible	Mutualy SSL; IPsec; IDS; Known BSP IP and URL
Replay	-	negligible	Time Anchor and Timestamp messages

Table 4. Construction of IDN.

<table>
<tr><th>Parameter</th><th>Values and Results</th></tr>
<tr><td><code>k</code></td><td>c2ec8d17c0ef9147af75814255513e56d27231fc73fdd27048240414fbbaa154</td></tr>
<tr><td><code>CPF</code></td><td>12345678901</td></tr>
<tr><td><code>TCN</code></td><td>3E59C8E1-F3D2-4F14-B03A-EA45EEF22627</td></tr>
<tr><td>CPFEXT</td><td>3132333435363738393031313233343536373839303131323334353637383930</td></tr>
<tr><td>K||CPFEXT</td><td>c2ec8d17c0ef9147af75814255513e56d27231fc73fdd27048240414fbbaa1543132333435363738393031313233343536373839303131323334353637383930</td></tr>
<tr><td>SHA256 (K||CPFEXT)</td><td>0f1d397e009f0f4813b953d5a7688a1f14606ad021d940a6c8ca97619ed2c042</td></tr>
<tr><td>A</td><td>0f1d397e009f0f4813b953d5a7688a1f</td></tr>
<tr><td>B</td><td>14606ad021d940a6c8ca97619ed2c042</td></tr>
<tr><td><code>iv</code></td><td>1b7d53ae21464feedb73c4b439ba4a5d</td></tr>
<tr><td>CPF Block</td><td>31323334353637383930310505050505 (padding)</td></tr>
<tr><td>ID</td><td>c162acd5c93b74e44f35af583d15f497</td></tr>
<tr><td>TCNEXT</td><td>33453539433845312D463344322D344631342D423033412D4541343545454632</td></tr>
<tr><td>K||TCNEXT</td><td>c2ec8d17c0ef9147af75814255513e56d27231fc73fdd27048240414fbbaa15433453539433845312D463344322D344631342D423033412D454134354545463</td></tr>
<tr><td>SHA256 (K||TCNEXT)</td><td>e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855</td></tr>
<tr><td>C</td><td>e3b0c44298fc1c149afbf4c8996fb924</td></tr>
<tr><td>D</td><td>27ae41e4649b934ca495991b7852b855</td></tr>
<tr><td><code>nonce</code></td><td>c41e85a6fc678f583e6e6dd3e13d0171</td></tr>
<tr><td>IDN</td><td>057c2973355cfbbc715bc28bdc28f5e6</td></tr>
</table>

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

with a `change_status` messages are shown.

[DIR:RECEIVED] FROM=BSP2; REQUEST=
{"requestType":"pending_operations"}

[DIR:SENT] TO=BSP2; RESULT=
{"pendingOperationsList":[{
"operationType":"1_n_queue",
"idnList":[{"idn":
"10d548f2fe7559d0a3162bc3db992ff2",
"tcn":0BB79BA3-2911-4297-9758-10E0
BF975002"}]}]}

[DIR:RECEIVED] FROM=BSP2; REQUEST=
{"requestType":"operation_resend","idn":
"10d548f2fe7559d0a3162bc3db992ff2",
"tcn":"0BB79BA3-2911-4297-9758-10E0BF97
5002"}

[DIR:SENT] TO=BSP2;RESULT=
{"response":``IDE","idn":
"10d548f2fe7559d0a3162bc3db992ff2",
"tcn":"0BB79BA3-2911-4297-9758-10E0BF97
5002"}

The `pending_operation` mechanism ensures that every BSP processes all data. By requesting it, the BSP 2 received from BSP 1 all the tuple IDN and `TCN` that were not processed. This command allows the network to be righteous, *i.e.*, without any missing identification processes. After, the BSP 2, which requested the `pending_operation` and received the IDN list, sent a `operation_resend`, that ensures BSP 1 that BSP 2 is ready to process the missing transactions. Immediately after indicating that BSP 2 is ready, the designated BSP 1 sent the `IDE` transactions.

[HUB:SENT] TO=BSP2;
REQUEST={"requestType":"z_query",
"idn":"66f5a1b3282da4ac74aabf28
112c240a","tcn":"0C490874-B4F5-
46ED-B9CB-BEB8E6F71081"}

[HUB:RECEIVED] FROM=BSP2;RESULT=
{``exists":``FALSE","idn":"66f5a1b3
282da4ac74aabf28112c240a",
"tcn":"0C490874-B4F5-46ED-B9CB
-BEB8E6F71081"

[HUB:SENT] TO=BSP2;TRANSACTION=
{"transaction-type":"IDE","idn":
"66f5a1b3282da4ac74aabf28112c240a",
"tcn":"0C490874-B4F5-46ED-B9CB
-BEB8E6F71081","timestamp":
"1575288144418"}

[HUB:RECEIVED] FROM=BSP2;TRANSACTION=
{"transaction-type":"VRE","idn":
"66f5a1b3282da4ac74aabf28112c240a",
"tcn":"02FA798D-D81F-43DB-9E44-32489
389C470","timestamp":"1575288144418",
"reference-tcn":"0C490874-B4F5-46ED
-B9CB-BEB8E6F71081","srf":"X"}

[HUB:SENT] TO=BSP2;REQUEST=
{"requestType":"change_status","idn":
"66f5a1b3282da4ac74aabf28112c240a";
"tcn":"0C490874-B4F5-46ED-B9CB-BEB8E6
F71081"}

Table 5. Principals' component settings.

Component	*BSP 1*	*BSP 2*
HSM	ASI-HSM AHX5 KNET Cryptographic Module	ASI-HSM AHX5 KNET Cryptographic Module
HUB/Directory Service O.S.	Linux Ubuntu 18.04	Linux CentOS 7
HUB/Directory Service Processors	Intel(R) Xeon (R) E5 - 2699	Intel(R) Xeon (R) E5-2650
Database	MongoDB	Apache Hbase
Link capacity	500/500 Mbps	500/500 Mbps

After running the local process, BSP 1 requests an `IDE` for the IDN "66f5a1..." to BSP 2. The BSP 2 responded a `VRE` with `X` value, *i.e.*, no biometrics were found in the biometric database. The BSP 1 sent a `change_status` acknowledge message, completing the registration process, and BSP 2 can store in its cache database. Every `IDE` request has attached the encrypted ANSI/NIST package with the biometrics corresponding to each IDN. Only the private key of each BSP can open the package and perform biometric identification processes. These results prove that the proposed scheme is secure, viable, and could be incorporated into IEEE BOPS to have biometric network flow integrity mechanisms.

D. PERFORMANCE OF THE PROPOSED SCHEME

We will comment on the performance of the proposed scheme. For this work, performance is the efficiency of the network in processing online transactions. The results are from a running instance between BSP 1 and BSP 2. First, in Table 5, we show the principals' components' settings used for this work. Then the HSM encrypts/decrypts capacity. Finally, we show the `IDE` and `pending_operations` numbers per day, running the API proposed over a week. The method applied to measure performance was to check how many `IDE` transactions BSP 1 sent and how many `pending_operations` transactions BSP 2 had per day. It means BSP 2's ability to process demand transactions within the scope of this paper.

The HSM performs a Conditional Self-Tests during its operation, according to FIPS. The nominal number to establish the script with AES-256-bits is over 1.000 per second. This performance is much higher than when the transactions are carried out by the proposed network. As will be shown, the HSM encryption capacity, using the suggested OpenSSL script, is much greater than the network's ability to send and receive transactions.

We measured the overall performance of the network for a week regarding `IDE` and `pending_operations` transactions. In Figure 5 and Figure 6 we show the results:

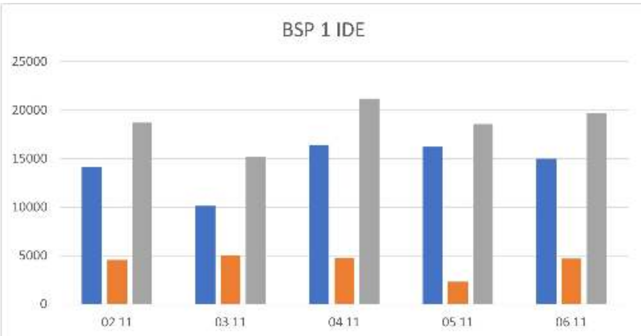


Figure 5. 1: IDE over a week.

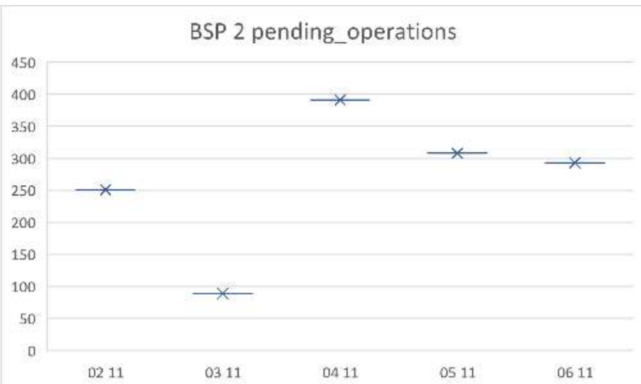


Figure 6. BSP 2: pending_operation over a week.

The BSP 1 sent an average of 14,389 `IDE` transactions per day and received from BSP 2 an average of 4,284 for the same JSON requests. The `pending_operations` that BSP 2 requests for BSP 1 have an average of 266 transactions per day. The proposed scheme's performance, given by $\frac{number of pending\_operations}{number of IDE}$, is approximately 98,15%.

VI. CONCLUSIONS

Security, privacy, and interoperability should be the main requirements of all implemented biometric networks. Biometric databases that communicate, or intend to do so, cannot guarantee a person's anonymity and yet complete the necessary processes to reliably identify an individual. Operating the systems under these circumstances leads to privacy and security failures, and this situation has to be changed. Besides, in light of recognition systems' interoperability based on different technological frameworks, no communication protocol fulfills the requirements for exchanging biometric data through the networks anonymously with a method that ensures transactions' integrity. We put forward a novel scheme that guarantees everyone's anonymity within the biometric databases and still allows them to communicate securely by following all the identification procedures. A probabilistic encryption scheme and a new communication protocol were used to achieve privacy, together with security evidence and interoperability to ensure the integrity of messages sent between biometric networks. We successfully produced an anonymous index for all the databases representing only one person for the same input data and secret key among the systems. However, we believe that the IEEE BOPS standard can be improved by establishing an additional framework for JSON messages between systems, including a way for networks to maintain their operations regardless of contingencies. In future work, it should be possible to expand the communication protocol for updated biometric packages. Moreover, the IDN algorithm that was created can provide security, privacy, and interoperability for general purposes, e.g., for any communication network or database segmentation, particularly those that use encryption schemes, like 5G security architecture. This future work will be a logical outcome of the contributions we have made to the new interoperability protocol, which involves sharing an encrypted index, enhancing security, and ensuring privacy for the biometric network.

.

APPENDIX A PROOF OF LEMMA 1

In order to perform formal analysis automatically of keys that are generated by the offline HSM, we used the NIST test suite [41]. We compiled the "make iid" and "make non_iid" tests using the "libdivsufsort-dev / libbz2-dev" dependencies, with a Ubuntu 18.04 operation system, with the following results:

```
NIST IID test

./ea_iid -i keys.bin
Calculating baseline statistics...
H_original: 7.886548
H_bitstring: 0.998301
min(H_original, 8 X H_bitstring):
7.886548
** Passed chi square tests
** Passed length of longest
repeated substring test
Beginning initial tests...
Beginning permutation tests... these
may take some time
** Passed IID permutation tests

NIST Non-IID test

./ea_non_iid -i keys.bin
Running non-IID tests...
Running Most Common Value Estimate...
Running Entropic Statistic Estimates
```

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access


```
(bit strings only)...
Running Tuple Estimates...
Running Predictor Estimates...
H_original: 7.718814
H_bitstring: 0.932005
min(H_original, 8 X H_bitstring):
7.456043
```

This result proves that the official NIST test suite approves the randomness of the keys (k) that are generated from the proposed scheme.

APPENDIX B API

We present the API code that can be emerged in IEEE BOPS. Each step determines which type of call is required in requests and responses for integrity purposes.


```
swagger: "2.0"
info:
  description: "API"
  version: "1.0.0"
  title: ""
  contact:
    email: "emlacerdaf@gmail.com"
tags:
- name: "directory"
  description: "Synchronous Pattern"
- name: "hub"
  description: "Asynchronous Pattern"

schemes:
- "https"

paths:
  /directory/zquery:
    get:
      tags:
      - directory
      description: "zquery"
      consumes:
      - application/json
      produces:
      - application/json
      parameters:
      - in: query
        name: z
        type: string
        required: true
        description: "zcode"
      responses:
        200:
          description: "z was found in
          the base"
          schema:
            $ref: "#/definitions/
        zquery"
        204:
          description: "z not found"
        400:
          description: "Bad request"
        401:
          description: "Request without
          certificate"
        403:
          description: "Certificate not
          recognize"

/directory/PendingOperations:
  get:
    tags:
    - directory
    description: "Pending-operations
    listing operation"
    consumes:
    - application/json
    produces:
    - application/json
    responses:
      200:
        description: "Return from
        pending-operations"
        schema:
          $ref: "#/definitions/
          PendingOperations"
      400:
        description: "Bad request"
      401:
        description: "Request without
        certificate"
      403:
        description: "Unrecognized
        certificate"

/directory/operation-resend:
  get:
    tags:
    - directory
    description: "Operation resubmit
    request pending-operation"
    consumes:
    - application/json
    produces:
    - application/json
    parameters:
    - in: query
      name: tcn
      type: string
      required: true
      description: "TCN code"
    responses:
      202:
        description: "Accepted"
      400:
```

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access


```
        description: "Bad request"
      401:
        description: "Request without
        certificate"
      403:
        description: "Unrecognized
        certificate"

/directory/idn-list:
  get:
    tags:
    - directory
    description: "IDN list"
    consumes:
    - application/json
    produces:
    - application/json
    parameters:
    - in: query
      name: startDate
      type: integer
      description: "UNIX Timestamp
      UTC"
    - in: query
      name: endDate
      description: "UNIX Timestamp
      UTC"
      type: integer
    responses:
      200:
        description: "OK"
        schema:
          $ref: "#/definitions
      /IdnList"
      400:
        description: "Bad request"
      401:
        description: "Request without
        certificate"
      403:
        description: "Unrecognized
        certificate"

/hub:
  post:
    tags:
    - Hub
    description: "Hub operations"
    consumes:
    - application/xml
    - application/octet-stream
    produces:
    - application/json
    parameters:
      - in: body
        name: NIST
        description: ANSI/NIST
      transaction
        schema:
          type: object
          example:
    responses:
      202:
        description: "Accepted"
      400:
        description: "Bad request"
        schema:
          $ref: "#/definitions
      /HubError"
      401:
        description: "Request without
        certificate"
      403:
        description: "Unrecognized
        certificate"

definitions:
  ZQuery:
    type: object
    properties:
      idn:
        type: string
        example: "IDN code"
      timestamp:
        type: integer
        example: 1234567890123
      exists:
        type: string
        example: "TRUE or FALSE"
      t_14_013_1:
        type: string
        example: "Corresponding TCN or
        blanck"
      t_14_013_2:
        type: string
        example: "TCorresponding TCN or
        blanck"
      t_14_013_3:
        type:  string
        example: "Corresponding TCN or
        blanck"
      t_14_013_4:
        type: string
        example: "Corresponding TCN or
        blanck"
      t_14_013_5:
        type: string
        example: "Corresponding TCN or
        blanck"
      t_14_013_6:
        type: string
        example: "Corresponding TCN or
```

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access


```
      blanck"
    t_14_013_7:
      type:  string
      example: "Corresponding TCN or
      blanck"
    t_14_013_8:
      type: string
      example: "Corresponding TCN or
      blanck"
    t_14_013_9:
      type: string
      example: "Corresponding TCN or
      blanck"
    t_14_013_10:
      type: string
      example: "Corresponding TCN or
      blanck"
    t_10:
      type: string
      example: "Corresponding TCN or
      blanck"

PendingOperations:
  type: object
  properties:
    pendingOperationsList:
      type: array
      maxItems: 1000
      items:
        type: string
      example:
      - "IDN of the pending
      transaction, TCN of the pending
      transaction"
      - "IDN of the pending
      transaction, TCN of the pending
      transaction"


idnList:
  type: array
  items:
    properties:
      idn:
        type: string
        example: ""
      timestamp:
        type: integer
        example: 1234567890123
      t_14_013_1:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_2:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_3:
        type:  string
        example: "Corresponding TCN
        or blanck"
      t_14_013_4:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_5:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_6:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_7:
        type:  string
        example: "Corresponding TCN
        or blanck"
      t_14_013_8:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_9:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_10:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_10:
        type: string
        example: "Corresponding TCN
        or blanck"

HubError:
  type: object
  properties:
    errorCode:
      type: integer
      example: 999
    errorMessage:
      type: string
      example: "error"
```

References

[1] A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016.

[2] P. T. J. Wolters, “The security of personal data under the GDPR: a harmonized duty or a shared responsibility?” *International Data Privacy Law*, vol. 7, no. 3, pp. 165–178, 2017. [Online]. Available:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

http://dx.doi.org/10.1093/idpl/ipx008

[3] J. Bustard, "The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 101–108, Sep. 2015.

[4] S. K. Choudhary and A. K. Naik, "Multimodal Biometric Authentication with Secured Templates — A Review," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, April 2019, pp. 1062–1069.

[5] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420, June 2018.

[6] M. Sandhya and M. Prasad, *Biometric Template Protection: A Systematic Literature Review of Approaches and Modalities*, 12 2016.

[7] D. C. L. Ngo, A. B. J. Teoh, and J. Hu, *Biometric Security*. United Kingdom: Cambridge Scholars Publishing, 2015.

[8] P. Campisi, *Security and Privacy in Biometrics*. Springer Publishing Company, Incorporated, 2013.

[9] A. Ross, J. Shah, and A. K. Jain, "From Template to Image: Reconstructing Fingerprints from Minutiae Points," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 544–560, April 2007.

[10] C.-A. Toli and B. Preneel, "Privacy-preserving biometric authentication model for e-finance applications," in *ICISSP*, 2018.

[11] K. Zhou and J. Ren, "PassBio: Privacy-Preserving User-Centric Biometric Authentication," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3050–3063, Dec 2018.

[12] A. Kumar and A. Kumar, "A Cell-Array-Based Multibiometric Cryptosystem," *IEEE Access*, vol. 4, pp. 15–25, 2016.

[13] C. Li, J. Hu, J. Pieprzyk, and W. Susilo, "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1193–1206, June 2015.

[14] M. Nasir and P. Perumal, "Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3297, 11 2013.

[15] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 255–268, Feb 2012.

[16] L. Lai, S. Ho, and H. V. Poor, "Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 122–139, March 2011.

[17] L. Lai, S. Ho, and H. V. Poor, "Privacy–Security Trade-Offs in Biometric Security Systems—Part II: Multiple Use Case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 140–151, March 2011.

[18] H. Kaur and P. Khanna, "Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 709–719, 2019.

[19] P. Punithavathi, S. Geetha, and S. Shanmugam, "Cloud-Based Framework for Cancelable Biometric System," in *2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, Nov 2017, pp. 35–38.

[20] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez, "Towards Cancelable Multi-Biometrics based on Bloom Filters: A Case Study on Feature Level Fusion of Face and Iris," in *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*, March 2015, pp. 1–6.

[21] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Mar. 2001. [Online]. Available: http://dx.doi.org/10.1147/sj.403.0614

[22] R. Tolosana, M. Gomez-Barrero, C. Busch, and J. Ortega-Garcia, "Biometric Presentation Attack Detection: Beyond the Visible Spectrum," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1261–1275, 2020.

[23] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of Privacy in Biometric Data," *IEEE Access*, vol. 4, pp. 880–892, 2016.

[24] T. Hirano, T. Ito, Y. Kawai, N. Matsuda, T. Yamamoto, and T. Munaka, "A Practical Attack to AINA2014's Countermeasure for Cancelable Biometric Authentication Protocols," in *2016 International Symposium on Information Theory and Its Applications (ISITA)*, Oct 2016, pp. 315–319.

[25] F. Quan, S. Fei, C. Anni, and Z. Feifei, "Cracking Cancelable Fingerprint Template of Ratha," in *2008 International Symposium on Computer Science and Computational Technology*, vol. 2, Dec 2008, pp. 572–575.

[26] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '96. London, UK, UK: Springer-Verlag, 1996, pp. 104–113. [Online]. Available: http://dl.acm.org/citation.cfm?id=646761.706156

[27] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, "Deep face representations for differential morphing attack detection," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3625–3639, 2020.

[28] IEEE, "IEEE Standard for Biometric Open Protocol, Redline," *IEEE Std 2410-2019 (Revision of IEEE Std 2410-2017), Redline*, pp. 1–134, June 2019.

[29] M. J. Dworkin, "SP 800-38A 2001 Edition. Recommendation for Block Cipher Modes of Operation: Methods and Techniques," Gaithersburg, MD, United States, Tech. Rep., 2001.

[30] K. B. Schaffer, "Security Requirements for Cryptographic Modules," pub-NIST, pub-NIST:adr, Federal Information Processing Standards Publication FIPS Pub 140-3, Mar. 2019.

[31] E. Rescorla, "HTTP Over TLS," RFC 2818, May 2000. [Online]. Available: https://rfc-editor.org/rfc/rfc2818.txt

[32] T. Bray, "The JavaScript Object Notation (JSON) Data Interchange Format," RFC 8259, Dec. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc8259.txt

[33] Q. Li and L. Zhang, "The Public Security and Personal Privacy Survey: Biometric Technology in Hong Kong," *IEEE Security Privacy*, vol. 14, no. 4, pp. 12–21, July 2016.

[34] C. Dwork, "Differential Privacy," in *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*, ser. ICALP'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1–12. [Online]. Available: http://dx.doi.org/10.1007/11787006_1

[35] M. Kaur and S. Sofat, "Fuzzy Vault template protection for Multimodal Biometric System," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, May 2017, pp. 1131–1135.

[36] K. Mangold, "Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information ANSI/NIST-ITL 1-2011 NIST Special Publication 500-290 Edition 3," no. 500-290e3, Aug. 2016, Special Publication (NIST SP).

[37] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification," *IEEE Access*, vol. 3, pp. 478–489, 2015.

[38] S. Mason, I. Gashi, L. Lugini, E. Marasco, and B. Cukic, "Interoperability between Fingerprint Biometric Systems: An Empirical Study," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, June 2014, pp. 586–597.

[39] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2," RFC 8017, Nov. 2016. [Online]. Available: https://rfc-editor.org/rfc/rfc8017.txt

[40] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption," in *Advances in Cryptology — EUROCRYPT'94*, A. De Santis, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 92–111.

[41] E. B. Turan, Meltem S.and Barker, K. Kelsey, J.and McKay, M. Baish, and M. Boyle, "SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation," Gaithersburg, MD, United States, Tech. Rep., 2018.

[42] O. Goldreich, *Foundations of Cryptography: Basic Tools*. New York, NY, USA: Cambridge University Press, 2000.

[43] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations Among Notions of Security for Public-key Encryption Schemes," in *Advances in Cryptology — CRYPTO '98*, H. Krawczyk, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 26–45.

[44] D. A. McGrew, "Impossible Plaintext Cryptanalysis and Probable-Plaintext Collision Attacks of 64-bit Block Cipher Modes," *IACR Cryptology ePrint Archive*, vol. 2012, p. 623, 2012.

[45] M. Bellare and T. Kohno, "Hash Function Balance and Its Impact on Birthday Attacks," in *Advances in Cryptology - EUROCRYPT 2004*, C. Cachin and J. L. Camenisch, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 401–418.

[46] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES," in *Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security*, ser. ASIACRYPT'11. Berlin,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3046630, IEEE Access

Heidelberg: Springer-Verlag, 2011, pp. 344–371. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-25385-0_19

[47] D. Khovratovich, C. Rechberger, and A. Savelieva, "Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family," in *Fast Software Encryption*, A. Canteaut, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 244–263.

[48] D. Khovratovich, "Bicliques for Permutations: Collision and Preimage Attacks in Stronger Settings," vol. 7658, 12 2012, pp. 544–561.

[49] P. Rogaway, "Evaluation of Some Blockcipher Modes of Operation," Evaluation carried out for the Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, Feb. 2011.

[50] H. Kang, M. Park, D. Moon, C. Lee, J. Kim, K. Kim, J. Kim, and S. Hong, "New Efficient Padding Methods Secure Against Padding Oracle Attacks," in *Information Security and Cryptology - ICISC 2015*, S. Kwon and A. Yun, Eds. Cham: Springer International Publishing, 2016, pp. 329–342.

[51] Y. Watanabe, J. Shikata, and H. Imai, "Equivalence Between Semantic Security and Indistinguishability Against Chosen Ciphertext Attacks," in *Public Key Cryptography — PKC 2003*, Y. G. Desmedt, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 71–84.

[52] Q. Dang, "Secure Hash Standard (SHS)," pub-NIST, pub-NIST:adr, Federal Information Processing Standards Publication FIPS Pub 180-4, Mar. 2015.

[53] A. Biryukov and D. Khovratovich, "Related-Key Cryptanalysis of the Full AES-192 and AES-256," in *Advances in Cryptology – ASIACRYPT 2009*, M. Matsui, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 1–18.

[54] E. B. Barker, W. C. Barker, W. E. Burr, W. T. Polk, and M. E. Smid, "SP 800-57 Part 1 Rev. 4. Recommendation for Key Management, Part 1: General," Gaithersburg, MD, United States, Tech. Rep., 2016.

[55] D. Bernstein and T. Lange, "Batch NFS," in *Selected Areas in Cryptography – SAC 2014: 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, ser. Lecture Notes in Computer Science, A. Joux and A. Youssef, Eds. Germany: Springer, 2014, pp. 38–58.

[56] J. Bonneau and I. Mironov, "Cache-Collision Timing Attacks Against AES," in *Cryptographic Hardware and Embedded Systems""CHES 2006*, ser. Lecture Notes in Computer Science, vol. 4249. Springer, October 2006, pp. 201–215. [Online]. Available: https://www.microsoft.com/en-us/research/publication/cache-collision-timing-attacks-against-aes/

[57] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[58] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," in *Advances in Cryptology — EUROCRYPT '97*, W. Fumy, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 37–51.

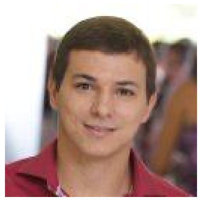
[59] Wenqian Yu, Weigang Li, Junyuan Wang, and Changzheng Wei, "A study of HSM based key protection in encryption file system," in *2016 IEEE Conference on Communications and Network Security (CNS)*, Oct 2016, pp. 352–353.

[60] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018. [Online]. Available: https://rfc-editor.org/rfc/rfc8446.txt

[61] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 01 2018.

[62] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 602–622, Firstquarter 2016.

EDUARDO M. LACERDA FILHO is a M. Sc. student in the Electrical Engineering Department (ENE) at the University of Brasilia (UnB). He received his B.S. degree from ENE/UnB in 2004. From 2004 to 2007, he was a Telecommunications Engineer Officer at Alcatel, responsible for technical specifications, reports, and studies aimed at 3G communications. Since 2007, he has been an Official Forensic Expert with the National Institute of Criminalistics, Brazil, where he has been involved in audio, video, and still image forensic analysis. He was requested to join the National Institute of Information and Technology, in 2011, where he is the Director of Public Key Infrastructure in Brazil. His research interests are cryptographic primitives and biometrics.



GERALDO P. ROCHA FILHO is an Assistant Professor at the Computer Science Department (CiC) at University of Brasılia (UnB). He received his Ph.D. in Computer Science from the University of São Paulo (USP) in 2018. He received his M.Sc. from the USP in 2014. He was also a post-doctoral research fellow at the Institute of Computing at UNICAMP before joining the UnB. His research interests are wireless sensor networks, vehicular networks, smart grids, smart home and machine learning.

RAFAEL TIMÓTEO DE SOUSA JÚNIOR (https://orcid.org/0000-0003-1101-3029) received his Bachelor Degree in Electrical Engineering, from the Federal University of Paraíba -– UFPB, Campina Grande, Brazil, 1984, his Master Degree in Computing and Information Systems, from the Ecole Supérieure d'Electricité -– Supélec, Rennes, France, 1984-1985, and his Doctorate Degree in Telecommunications and Signal Processing, from the University of Rennes 1, Rennes, France, 1988. He was a visiting researcher with the Group for Security of Information Systems and Networks (SSIR) at the Ecole Supérieure d'Electricité – Supélec, Rennes, France, 2006-2007. He worked in the private sector from 1988 to 1996. Since 1996, He is a Network Engineering Associate Professor with the Electrical Engineering Department, at the University of Brasília – UnB, Brazil, where he is the Coordinator of the Professional Post-Graduate Program on Electrical Engineering (PPEE) and supervises the Decision Technologies Laboratory (LATITUDE). He is Chair of the IEEE VTS Centro-Norte Brasil Chapter (IEEE VTS Chapter of the Year 2019) and of the IEEE Centro-Norte Brasil Blockchain Group. His professional experience includes research projects with Dell Computers, HP, IBM, Cisco, and Siemens. He has coordinated research, development, and technology transfer projects with the Brazilian Ministries of Planning, Economy, and Justice, as well as with the Institutional Security Office of the Presidency of Brazil, the Administrative Council for Economic Defense, the General Attorney of the Union and the Brazilian Union Public Defender. He has received research grants from the Brazilian research and innovation agencies CNPq, CAPES, FINEP, RNP, and FAPDF. He has developed research in cyber, information and network security, distributed data services and machine learning for intrusion and fraud detection, as well as signal processing, energy harvesting and security at the physical layer.

VINÍCIUS P. GONÇALVES (https://orcid.org/0000-0002-3771-2605) has a Ph.D. in Computer Science and Computational Mathematics (2016) from the University of São Paulo (USP). He was also a research fellow at the University of Arizona (USA) before joining the University of Brasília (UnB). Dr. Gonçalves was a Postdoctoral Researcher at the USP Medical School, with a CAPES Fellowship. Currently, he is an Assistant Professor in the Electrical Engineering Department (ENE) at UnB, Brasília, Brazil, where he is a member of the Graduate Programs in Electrical Engineering (PPGEE and PPEE). Dr. Gonçalves is a researcher and member of the AQUARELA Group; his main research interests include Human–Computer Interaction, Internet of Things, Cybersecurity, Mobile Health, Image Processing and Machine Learning.

• • •